

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

– against –

HALIMA SALMAN,

*Defendant.*

**MEMORANDUM & ORDER**  
24-cr-00206 (NCM)

**NATASHA C. MERLE**, United States District Judge:

Defendant Halima Salman is charged with receiving military type training from a foreign terrorist organization in violation of Title 18, United States Code, Section 2339D. *See* Indictment, ECF No. 13. Before the Court is defendant’s pretrial motion to suppress evidence obtained through queries of the National Media Exploitation Center (“NMEC”) database, or, in the alternative, an evidentiary hearing as to the admissibility of such evidence. *See* Motion to Suppress (“Mot.”), ECF No. 76. For the reasons stated below, defendant’s motion is denied.

**BACKGROUND**

Salman has been charged under Section 2339D based, at least in part, on evidence obtained through the government’s warrantless querying of the NMEC database. This evidence includes a military training document (“Military Training Document”) which contains the defendant’s alias—or “kunya”—Um Khattab al-Muhajir, and photographs

and video of defendant.<sup>1</sup> The government argues that the evidence obtained from the NMEC database supports that the defendant did, indeed, receive military type training from the Islamic State of Iraq and al-Sham (“ISIS”). Defendant contests the authenticity of the training document, but for purposes of this motion, what is important is that the document, video, and photographs were obtained in response to queries by the government of information in the NMEC database.

What is the NMEC database? As articulated by defendant, it is a “massive database of digital media and personal information that the government has acquired, seized, or captured outside of the United States.” Mot. 5.<sup>2</sup> Defendant states that the Federal Bureau of Investigation (“FBI”) has been involved with NMEC since its inception in 2003 for the purpose of assisting law enforcement and counterterrorism prosecutions in the United States. Mot. 10 n.4. The government explains that the NMEC database contains Collected Exploitable Material (“CEM”), which is information that includes, but is not limited to, material seized or captured during or following United States military, law enforcement, or other government agency engagements outside the United States, and materials provided by foreign militaries or law enforcement officials outside the United States to United States authorities. *See* Government’s Opposition (“Opp’n”) 24, ECF No. 80.<sup>3</sup> As

---

<sup>1</sup> Defendant characterizes a kunya as a nickname but does not deny that the name contained in the Military Training Document is her kunya. Reply 86; *see also* Oral Arg. Tr. 6:5–6.

<sup>2</sup> Throughout this Order, page numbers for docket filings refer to the page numbers assigned in ECF filing headers.

<sup>3</sup> The Court does not have significant information about the NMEC database, including its size or the types of information it may contain. Defendant requested such information about the size, the types of files, and the number of records about U.S. citizens contained in the NMEC database in her motion to compel. *See* ECF Nos. 85, 101.

relevant here, a physical device captured on foreign battlefields may be transferred to a Regional Exploitation Center (“REC”), where the device is “exploited” by creating a “gold copy” or a bit-for-bit copy, that is then transmitted to NMEC. Opp’n 24.

Relevant here, two phones belonging to Salman’s husband, Abu Ali, were seized in Syria, and the contents of his phones were uploaded to the NMEC database. The government states that the information at issue here originated from two phones that were confiscated from Abu Ali by the Syrian Democratic Forces, after which they eventually came into possession of the United States and were transported to an REC in Iraq, where the data from the phones was exploited and transferred to NMEC. *See* Opp’n 25–26. The contents of the phones included the Military Training Document, as well as a video and pictures of Salman.

As for the search of the NMEC database, the government states that in July 2022, the FBI ran a search in a system called Harmony, which is a “platform for the dissemination of information between agencies in the intelligence community,” and which contains “a small percentage of the extractions available at NMEC.” Opp’n 26. The query used to search Harmony was the name of an investigative subject who is not the defendant. Among the search results was a “photobook” from one of the Abu Ali phones that contained photographs of defendant. Opp’n 26–27. The FBI thereafter requested the gold copy of each Abu Ali phone from NMEC. Opp’n 27. The gold copies contained additional photos of defendant, including photos with the ISIS flag and with an AK-47 style rifle in the background. Opp’n 27. The gold copy also allegedly contained a video of

---

In response, the government represents that it does not possess records responsive to these requests. ECF No. 102 at 3. Nevertheless, as the Court finds that defendant has failed to articulate a privacy interest in any of the information contained in the database, this information is unnecessary for the Court to resolve the instant motion.

the defendant holding an AK-47. Opp’n 28. One of the phones also contained the Military Training Document in Arabic. Opp’n 31 n.5. In June 2023, the government represents that the FBI requested updated searches of defendant’s husband’s true name: Mati’allah Bin Abdallah Nurzad, from “the CEM extractions within the United States’s holdings of CEM.” Opp’n 30. The government thus represents that the evidence of defendant’s alleged military training with ISIS was returned based on searches related to the defendant’s husband and another investigative subject, and that searches that returned the information at issue in this motion did not name defendant. Opp’n 31; Oral Arg. Tr. 77:19–24, ECF No. 117.

Defendant argues that evidence obtained through the government’s warrantless queries of the NMEC database should be suppressed. *See generally* Mot. Defendant does not challenge the reasonableness of the initial collection of the data here at issue, i.e., the seizure of Abu Ali’s phones in Syria and the extraction of the data, *see* Mot. 10 n.4, instead, she argues that querying the NMEC database constitutes a Fourth Amendment event for which the government should have obtained a warrant, *see* Mot. 14.

## DISCUSSION

### I. Fourth Amendment Jurisprudence

The “touchstone” of a Fourth Amendment inquiry “is the question whether a person has a constitutionally protected reasonable expectation of privacy.” *United States v. Gori*, 230 F.3d 44, 50 (2d Cir. 2000) (quoting *Oliver v. United States*, 466 U.S. 170, 177 (1984)).<sup>4</sup> Thus, the first step in evaluating a Fourth Amendment challenge is a determination of whether the defendant had a legitimate expectation of privacy in the

---

<sup>4</sup> Throughout this Order, the Court omits all internal quotation marks, footnotes, and citations, and adopts all alterations, unless otherwise indicated.

thing or place being searched. *See United States v. Hamilton*, 538 F.3d 162, 167 (2d Cir. 2008). This inquiry involves two distinct questions: “first, whether the individual had a subjective expectation of privacy; and second, whether that expectation of privacy is one that society accepts as reasonable.” *Id.* Although “no single rubric definitively resolves which expectations of privacy are entitled to protection,” *Carpenter v. United States*, 585 U.S. 296, 304 (2018), in determining the privacy expectations that society is prepared to accept as reasonable, the Supreme Court has “given weight to such factors as the intention of the Framers of the Fourth Amendment, the uses to which the individual has put a location, and our societal understanding that certain areas deserve the most scrupulous protection from government invasion.” *O’Connor v. Ortega*, 480 U.S. 709, 715 (1987).

A defendant has standing to bring a Fourth Amendment suppression motion when challenged conduct has invaded her reasonable expectation of privacy in a place or object searched. *United States v. Ephron*, No. 24-cr-00418, 2025 WL 524027, at \*5 (S.D.N.Y. Feb. 18, 2025) (“[T]he touchstone of Fourth Amendment standing is whether the person challenging the search has a reasonable expectation of privacy in the place that was searched; in other words, a privacy interest that society is prepared to recognize as reasonable.”); *see also United States v. Alcantara*, No. 22-cr-00152, 2023 WL 3883961, at \*3 (S.D.N.Y. June 8, 2023) (“[A] defendant asking a court to suppress evidence must demonstrate a legitimate expectation of privacy in the area that was searched.”). Thus, the concept of “standing in Fourth Amendment cases can be a useful shorthand for capturing the idea that a person must have a cognizable Fourth Amendment interest . . . before seeking relief for an unconstitutional search.” *Byrd v. United States*, 584 U.S. 395, 410 (2018). That is, standing under the Fourth Amendment is not a “jurisdictional question; it is fundamental to the determination of whether a Fourth

Amendment violation occurred.” *United States v. Nelson*, No. 20-cr-00353, 2022 WL 18636591, at \*5 (E.D.N.Y. Oct. 24, 2022), *report and recommendation adopted in part*, 2023 WL 358421 (Jan. 23, 2023). Under the Fourth Amendment, a defendant does not have standing to move to suppress the results of a search if she does not have a privacy interest in the thing or place being searched, even if the search targeted the defendant. *See Rakas v. Illinois*, 439 U.S. 128, 132–34 (1978) (rejecting argument that an individual who was the “target” of a search would have standing to contest the legality of the search, and reaffirming that Fourth Amendment rights are personal rights that may not be asserted vicariously); *see also United States v. Serrano*, 695 F. App’x 20, 23 (2d Cir. 2017) (summary order) (“In order to prevail on a contention that a search violated the Fourth Amendment, an accused must show that [she] had a legitimate expectation of privacy in a searched place or item.”).

*A. Salman Has Not Established an Expectation of Privacy in the Searched Phones or in the Images Stored on the Searched Phones.*

Given there can be no standing to challenge a Fourth Amendment search that may have occurred without a reasonable expectation of privacy in the place or thing searched, that is where the Court begins—assessing whether Salman had a reasonable expectation of privacy in the NMEC database, the information contained therein, or in her husband’s phones that were uploaded to the NMEC database. The Court finds that defendant has not established a reasonable expectation of privacy in any.

The parties do not dispute that the information defendant seeks to suppress was uploaded to the NMEC database from two cell phones that did not belong to her. *See* Mot. 9 (noting that the photographs offered in the Complaint appear to have been collected by the extraction of a cell phone belonging to someone other than defendant); Compl. ¶ 20,

ECF No. 1 (“Based upon information found in NMEC’s databases . . . there is a cellular device recovered in Syria that the FBI assesses was used by Individual-3 . . . and that contains information relating to . . . [defendant’s] conduct[.]”). The government argues that the “search” which can be challenged occurred with the seizure and extraction of information from the phones. Oral Arg. Tr. 67:22–24, 68:6–10 (“The search is the extraction of the phone.”). According to the government, defendant has failed to establish “standing to seek suppression under the Fourth Amendment” because she does not have a reasonable expectation of privacy in the information contained on the Abu Ali phones. Opp’n 60. Defendant counters that she has an expectation of privacy in the information obtained from the NMEC database queries for two reasons: first, because some of the information in the database contained her private communications, and second, because some of the data in the database may have contained the contents of her own cell phone. Mot. 9. Both of defendant’s arguments as to her privacy interest fail.

- i. Salman has not articulated a reasonable expectation of privacy in her husband’s phones.

Defendant claims that the Abu Ali phones, and thus the NMEC database, “contained her private communications” which is evidenced from “the three selfies” of her offered in the complaint. Mot. 9. Specifically, Salman argues that the photographs were “electronic communications” that were either sent to or taken by Abu Ali’s phones. Therefore, defendant argues, these private communications give rise to a reasonable expectation of privacy, and she has Fourth Amendment standing to move to suppress the information which was contained on the Abu Ali phones. Mot. 8 n.3. This argument is unavailing.

First, assuming the photographs were taken by one of the Abu Ali phones, defendant does not have a privacy interest in the contents of a phone that does not belong to her. Defendant argues that the photographs contained on the phone constituted “electronic communications,” regardless of whether the photographs were “sent to or taken by” the Abu Ali phones. Mot. 9. However, defendant does not clearly articulate how a photograph taken by one device and stored on that device, without being sent to any other device, can constitute a “communication.” Assuming that the photographs were taken by one or both of the Abu Ali phones, these are simply photographs taken by and stored on a phone not belonging to defendant, in which she does not have an expectation of privacy. *See United States v. Salaman*, 742 F. Supp. 3d 221, 237 (D. Conn. 2024) (“To the extent that [defendant] complains that the warrant allowed for the seizure or search of other people’s cellphones, he has no standing to assert the Fourth Amendment rights of third parties.”).

Next, assuming that the photographs were taken by another device and sent to the Abu Ali phones,<sup>5</sup> a person does not have a reasonable expectation of privacy in another individual’s *phone* simply because she sent a “communication” to that phone. *See United States v. Lustyik*, 57 F. Supp. 3d 213, 223 (S.D.N.Y. 2014) (denying Fourth Amendment challenge of search of another person’s email account, and finding that the defendant lacked “an expectation of privacy both in [the third-party’s] email account and in any of

---

<sup>5</sup> Defendant provides no basis on which the Court should conclude that the photographs were taken on another device and sent to the Abu Ali phones. Defendant has not filed an affidavit or sworn statement establishing she took the photos on another device and sent them to one of the Abu Ali phones. *See United States v. Ulbricht*, No. 14-cr-00068, 2014 WL 5090039, at \*6 (S.D.N.Y. Oct. 10, 2014), *aff’d*, 858 F.3d 71 (2d Cir. 2017) (finding that a defendant’s expectation of privacy must “be established by a declaration or other affirmative statement of the person seeking to vindicate his or her personal Fourth Amendment interest in the thing or place searched”).

[the defendant's] emails received by [the third party]"). Thus, the fact that defendant may have taken the selfies on another device and sent them to one of her husband's phones does not give rise to an expectation of privacy in the receiving phone.

Additionally, to the extent defendant argues that she had a reasonable expectation of privacy in her husband's phones due to her use of those phones, this argument fails. *See* Mot. 9 (arguing that Salman had an expectation of privacy because the three selfies of Salman were "electronic communications, either sent to *or taken by the device*") (emphasis added). Defendant has not submitted an affidavit or other evidence to show that the phones were shared devices between herself and her husband, or that she used her husband's phones to such an extent that she had a subjective expectation of privacy in them. *See United States v. Dore*, 586 F. App'x 42, 46 (2d Cir. 2014) (summary order) ("[Defendant] did not submit an affidavit establishing that the cell phones in question belonged to him or that he had a subjective expectation of privacy in them. Nor did [defendant] assert a privacy interest in the cell phones in some other manner. Consequently, [defendant] does not have standing to assert Fourth Amendment rights in those phone records."); *United States v. Walker*, No. 16-cr-00567, slip op. 5–6 (S.D.N.Y. Mar. 8, 2017), ECF No. 56 (affidavit from the defendant stating that he used the target cell phone "on occasion" insufficient to establish standing because "[a]t most, the defendant has demonstrated non-exclusive and sporadic use" of the cell phone at issue). Defendant has not argued that she used or saved personal information on the phones to such an extent that she had a reasonable expectation of privacy in the phones. *See United States v. Santillan*, 902 F.3d 49, 62 (2d Cir. 2018) ("One need not be the owner of the property for [her] privacy interest to be one that the Fourth Amendment protects, so long as [she] has the right to exclude others from dealing with the property.").

Accordingly, defendant has not established a reasonable expectation of privacy in the phones.

- ii. Salman has not articulated a reasonable expectation of privacy in the images stored on the Abu Ali phones.

Next, if the Court were to assess whether defendant had a privacy interest in the images stored on the phone themselves, rather than the device from which they were retrieved, this argument also fails. Salman does not explain how a photograph being taken and saved on an Abu Ali phone, or taken on a different device and sent to an Abu Ali phone, conveys a reasonable expectation of privacy in the photograph. Defendant simply contends that she has an “expectation of privacy in . . . her electronic communications,” as “[t]exting a selfie is no different, constitutionally speaking, from sending an email.” Mot. 10.

To begin, defendant has not established through a sworn statement or any other evidence that she did, in fact, text a selfie to one of the Abu Ali phones. However, assuming that the images of Salman were captured with another device and sent to Abu Ali’s phones, presumably by defendant, that communication does not necessarily retain a reasonable expectation of privacy after its transmission, storage, and eventual collection from the Abu Ali phones.

This conclusion arises from the well-established “third-party” doctrine, under which a person has “no legitimate expectation of privacy in information [she] voluntarily turns over to third parties.” *Carpenter*, 585 U.S. at 308; *see also United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) (noting that while individuals generally possess a reasonable expectation of privacy in their home computer, they “may not, however, enjoy such an expectation of privacy in transmissions over the Internet or e-mail that have

already arrived at the recipient”); *Ulbricht*, 2014 WL 5090039, at \*13 (“It also seems likely that many of [defendant’s] emails were to individuals other than himself, which could defeat an expectation of privacy in them.”); *United States v. Zottola*, No. 18-cr-00609, 2022 WL 3682222, at \*6 (E.D.N.Y. Aug. 25, 2022) (“[Defendant] voluntarily sent messages to [a third-party], which were stored on [the third-party’s] phone. [Defendant] therefore has no legitimate expectation of privacy in the data he sent to [the third-party] and lacks standing to seek its suppression.”). Here, assuming defendant sent the photographs to the retrieved device, given that they had been shared with a third party, defendant assumed the risk that the photos would be shared with others. Thus, the fact that she sent the “communication” to the retrieved device does not establish—and in fact, undermines—an inference that defendant had an expectation of privacy in the photos.

Accordingly, defendant has failed to articulate a basis on which the Court could conclude that she had a subjective expectation of privacy in the images and video contained on the Abu Ali phones, *see Ulbricht*, 2014 WL 5090039, at \*13 (noting that “[t]he Court cannot just assume a subjective expectation of privacy”), nor has she established that any subjective expectation of privacy in those selfies is one that society is prepared to accept as reasonable.

- iii. Salman has not established that any of the information stored in the NMEC database came from a device in which she has a reasonable expectation of privacy.

Lastly, defendant states in her motion that “upon information and belief, the Syrian [Democratic] Forces, working together with the U.S. military, seized a cell phone from Salman in March 2019,” and thus “there is a reasonable probability that Salman’s cell phone contents were in the NMEC database queried.” Mot. 9. However, there is no indication in the record before the Court, or presented by Salman, that any information

was extracted from defendant's phone and stored in NMEC or that any information extracted from NMEC was originally (and only) contained on defendant's phone. *See* Compl. ¶¶ 20–28. Indeed, in her reply brief, defendant concedes that “the evidence discovered by searching the NMEC database did not come from an extraction of Salman's cell phone.” Reply 33. Speculation as to whether Salman's phone was searched is not adequate to establish that she has a privacy interest in the information obtained from the NMEC database.

\* \* \*

As defendant has failed to establish that she had a reasonable expectation of privacy in the phones which were uploaded to the NMEC database, and which contained the information she seeks to suppress, or in any of the information uploaded to the NMEC database, defendant lacks standing to bring a Fourth Amendment suppression challenge.<sup>6</sup>

*B. Querying the NMEC Database Alone Does Not Confer a Privacy Interest to Salman.*

Notwithstanding her lack of a privacy interest in the Abu Ali phones, or the photographs and video contained therein, Salman clarifies in her reply brief that she “does not ask to suppress the seizure or search of any third-party's cell phone.” Reply 33. Instead, defendant seeks to “suppress the search results from a massive government

---

<sup>6</sup> Defendant has also failed to show that she is entitled to an evidentiary hearing on her motion. “Unless a defendant makes a sufficiently definite, specific, detailed, and nonconjectural showing that there is a contested issue of material fact, they are not entitled to an evidentiary hearing.” *Alcantara*, 2023 WL 3883961, at \*5 (quoting *United States v. Pena*, 961 F.2d 333, 339 (2d Cir. 1992)). To raise a material issue of fact, a defendant must file an affidavit of someone with personal knowledge. *Id.* While defendant requests an evidentiary hearing, she does not identify facts at issue, nor has she filed an affidavit in support of her motion. Thus, defendant's alternative request for an evidentiary hearing on this motion is denied.

database containing 20 years' worth of device extractions and documents obtained by the United States intelligence community.” Reply 33; *see also* Oral Arg. Tr. 63:13–14. Put differently, defendant is challenging “the querying of the NMEC database . . . to obtain information about a United States citizen for purposes of domestic prosecution.” Reply 39. Thus, defendant argues that she has standing to challenge queries of the NMEC database as long as those queries were related to her, regardless of whether she has an expectation of privacy in the underlying data contained in the database, or in the devices which were uploaded to the database.<sup>7</sup> The Court disagrees.

In support of her argument, defendant relies heavily on the Second Circuit’s decision in *United States v. Hasbajrami* (“*Hasbajrami II*”), 945 F.3d 641 (2d Cir. 2019). Thus, it is helpful to recount the facts and holding of *Hasbajrami II*.

i. *Hasbajrami II*

*Hasbajrami II* concerned the warrantless querying of information collected and stored pursuant to Section 702 of the Foreign Intelligence Surveillance Act (“FISA”). In that case, the queries returned incidental or inadvertent communications (including incriminating communications) that a United States citizen, the defendant in that case, had with individuals without ties to the United States and located abroad. *Hasbajrami II*,

---

<sup>7</sup> The NMEC database, and the queries of the database that returned the information at issue in this motion, are also a subject of defendant’s motion to compel discovery. *See* Motion to Compel Discovery, ECF No. 85. The Court has not yet ruled on those discovery requests, and indeed, need not given the Court’s denial of the instant motion. Nevertheless, the government has also represented that the queries that included Salman’s name did not return any of the information at issue in this motion. Oral Arg. Tr. 77:7–24. Additionally, the government has represented that the queries which returned the images of Salman and the Military Training Document were of the names of Salman’s husband and another investigative subject. Opp’n 31.

945 F.3d at 645. In that order, the court assessed whether querying a database could violate the Fourth Amendment, and held that it could. *Id.* at 646.

FISA traditionally governs surveillance inside the United States in the context of national security investigations. *Id.* at 650. “For those national security investigations, FISA established procedures governing the collection of information” derived from, among other things, electronic surveillance and the use of information so obtained. *Id.* In 2008, FISA was amended with the FISA Amendments Act to enact Section 702, in response to concern about the limitations of FISA in conducting national security investigations following the September 11, 2001 attacks. *Id.* at 650–51. Specifically, traditional FISA applications required a court order, thus requiring probable cause, which the government believed restricted the speed necessary to detect and respond to terrorist threats.

Under Section 702, the government may conduct electronic surveillance of targets, without an individualized probable cause determination, where the government reasonably believes that the targeted person is located outside of the United States. *Id.* at 651–52. The electronic surveillance enabled by FISA allows the government to intercept and review emails being sent to and from a target’s email account roughly in real time and therefore resembles a “traditional domestic law enforcement wiretap.” *Id.* at 653. Thus, under Section 702, the government can obtain emails or other electronic communications “to, from, or about individuals the government believes are (a) not United States persons and (b) located abroad.” *Id.* at 651.

The court concluded that no warrant was required for the government’s incidental collection of the communications of United States persons pursuant to Section 702 surveillance. *Id.* at 662–63. The court found that a warrant was not required first because

the Fourth Amendment does not apply extraterritorially, and thus the “warrantless surveillance of foreign individuals abroad under the circumstances that existed” in that case “present[ed] no cognizable constitutional problem.” *Id.* at 663. Next, the court concluded that the Fourth Amendment was not violated where law enforcement officers, having lawfully undertaken surveillance under an exception to the warrant requirement, “discover and seize either evidence of criminal activity that they would not have had probable cause to search for in the first place, or the relevant conversations of an individual they did not anticipate or name in a warrant application.” *Id.* at 663. Accordingly, the court held that the government “may lawfully collect, without a warrant and pursuant to Section 702, the e-mails of foreign individuals located abroad who reasonably appear to constitute a potential threat to the United States and, once it is lawfully collecting those e-mails, it does not need to seek a warrant, supported by probable cause, to continue to collect e-mails between that person and other individuals once it is learned that some of those individuals are United States citizens or lawful permanent residents, or are located in the United States.” *Id.* at 664.

Though a warrant may not have been required, the Second Circuit reaffirmed that the government’s actions must still be reasonable to be consistent with the Fourth Amendment. *Id.* at 666. The court “assume[d] that a United States person ordinarily has a reasonable expectation in the privacy of his e-mails sufficient to trigger a Fourth Amendment reasonableness inquiry when the government undertakes to monitor even foreign communications in a way that can be expected to, and in fact does, lead to the interception of communications with United States persons.” *Id.* at 666. The court then weighed Hasbajrami’s privacy interest with the government’s concern for national

security and found that such collection was reasonable under the Fourth Amendment. *Id.* at 667–68.

In *Hasbajrami II*, the court went on to address another issue: “the storage of Section 702 information in databases and the subsequent querying of those databases by the government.” *Id.* at 669. It is the analysis of this issue upon which Salman so heavily relies. The court noted that “storage and querying of information raises challenging constitutional questions, to which there are few [cl]ear answers in the case law.” *Id.* at 670. Traditionally, where criminal investigators reexamine evidence that has been lawfully seized, “such investigative steps” are not ordinarily considered to be “a new Fourth Amendment event.” *United States v. Johnson*, 93 F.4th 605, 613 (2d Cir. 2024), *cert. denied*, 145 S. Ct. 276 (2024). However, in the digital age, “the seizure of electronic devices [] can give the government possession of a vast trove of personal information,” and therefore is “very different from the seizure of a drug ledger or an item of clothing.” *Id.* Thus, the “mere fact that digital material has been lawfully collected does not in all circumstances permit the future review of stored information.” *Id.*

The *Hasbajrami II* Court concluded that queries related to the defendant of data stored pursuant to Section 702 had Fourth Amendment implications that “counsel[led] in favor of considering querying a separate Fourth Amendment event that, in itself, must be reasonable.” *Hasbajrami II*, 945 F.3d at 670. Those implications were as follows: first, courts have “increasingly recognized the need for additional probable cause or reasonableness assessments to support a search of information or objects that the government has lawfully collected”; second, the Section 702 database is “sweeping in its technological capacity and broad in its scope” such that the collections at issue could be analogized to traditional domestic criminal wiretapping; and third, querying may “make

it easier to target wide-ranging information about a given United States person at a point when the government knows it is investigating such a person.” *Id.* at 670–72. Finally, the court also noted that there is a “potentially significant difference between, for example, the FBI querying its own database and the FBI requesting that the NSA query its far larger archive of collected communications.” *Id.* at 672.

ii. Application of *Hasbajrami II* to NMEC Database Query

In light of *Hasbajrami II*, defendant seeks to place before the Court an as-yet unanswered question: whether the Second Circuit’s holding in *Hasbajrami II* that queries of stored Section 702 data can constitute a Fourth Amendment event applies to databases which contain non-Section 702 data. Defendant argues that the “same rule should apply to querying the NMEC database for information about U.S. persons such as Salman.” Mot. 8. The government in opposition argues that the Second Circuit’s determination in *Hasbajrami II* is unique to the Section 702 context. *See* Opp’n 63.

Defendant argues that she has standing to challenge the results of queries of the NMEC database so long as the queries of the database were related to her, and it “does not matter that the evidence discovered by searching the NMEC database did not come from an extraction of Salman’s cell phone.” Reply 33. At bottom, Salman seems to be arguing that even if she did not have a privacy interest in the information when it was deposited into NMEC, the act of storing information in NMEC conferred a privacy interest onto her. Defendant’s argument presupposes that *Hasbajrami II* held that a query about a person, or subjects related to a person, in a database that is “so big and different,” gives that person Fourth Amendment standing in and of itself. Oral Arg. Tr. 57:23–25. In fact, at oral argument, defense counsel argued that if the government “ran queries for [defendant’s] family members seeking information about [defendant],” those queries

would implicate the defendant's Fourth Amendment rights. Oral Arg. Tr. 61:6–9. However, the case law does not support this proposition. The Court does not agree that searching a database using queries that target a person, without any indication that the person being targeted has an expectation of privacy in anything contained in the database, gives that person standing to challenge the results of those queries under the Fourth Amendment. *See Rakas*, 439 U.S. at 132–34 (declining to “extend the rule of standing in Fourth Amendment cases” to allow “any criminal defendant at whom a search was directed . . . to contest the legality of that search and object to the admission at trial of evidence obtained as a result of the search”).

As stated above, *Hasbajrami II* concerned a legal permanent resident located in the United States whose emails were intercepted and provided to the government by internet service providers incidental to the surveillance of non-U.S. targets of 702 surveillance. *Id.* at 645–46, 654 (explaining that the “vast majority of Section 702 surveillance” at issue in the case was incidental, and that incidental surveillance can occur where a United States person emails a targeted individual and an internet service provider provides such emails to the National Security Agency). As discussed, pursuant to the “third-party” doctrine, a person generally has “no legitimate expectation of privacy in information [she] voluntarily turns over to third parties.” *Carpenter*, 585 U.S. at 307–08. When addressing the issue of the defendant's privacy interests in his electronic communications, in the district court order being appealed in *Hasbajrami II*, the district court concluded that the defendant had an expectation of privacy in his emails with non-U.S. persons located abroad. *See United States v. Hasbajrami* (“*Hasbajrami I*”), No. 11-cr-00623, 2016 WL 1029500, at \*10 (E.D.N.Y. Mar. 8, 2016). The district court reached this conclusion even though the defendant's expectation of privacy was “diminished”

because the emails had necessarily been shared with someone else, and the defendant had thus “assume[d] the risk that the recipient will share the communication with others.” *Id.* In so finding, the district court determined the third-party doctrine was less applicable in a case “concern[ing] government *interception* of emails.” *Hasbajrami I*, at \*11. The district court distinguished between those cases where the government collected the communication directly from the recipient of the communication, and where the government intercepts communications as they are flowing between sender and recipient. *Id.* at \*11. The Section 702 surveillance at issue in *Hasbajrami* allows the government to demand email communications directly from internet service providers, rather than a third-party recipient of an email communication. *Hasbajrami II*, 945 F.3d at 653.

On appeal, the Second Circuit assumed, without holding, that a “United States person ordinarily has a reasonable expectation in the privacy of his e-mails sufficient to trigger a Fourth Amendment reasonableness inquiry[.]” *Id.* at 666. Thus, rather than finding that querying a database for an individual, or for information about an individual, *creates* standing to make a Fourth Amendment challenge by itself, the Second Circuit held that once an individual has an expectation of privacy in the information contained in a database, further querying of the database for information related to the individual may be a Fourth Amendment event that must be reasonable. *See id.* (“For the purposes of *Hasbajrami*’s appeal, we may assume that a United States person ordinarily has a reasonable expectation in the privacy of his e-mails sufficient to trigger a Fourth Amendment reasonableness inquiry when the government undertakes to monitor even foreign communications in a way that can be expected to, and in fact does, lead to the interception of communications with United States persons.”).

As a threshold matter, and as discussed above, Salman has not established an expectation of privacy in any information at issue here. First, defendant has not established that any of the information at issue in this motion was actually sent by her to either of her husband's phones. Moreover, even if she had established that the information was contained on the phone because she had sent it to an Abu Ali phone, the government collected the information through the seizure and extraction of the phone itself, rather than through the interception of any communication. Thus, assuming she sent the information to the Abu Ali phone, this transmission implicates the third-party doctrine and undermines Salman's argument as to any expectation of privacy in "communications" sent to and stored on the devices.

Even if interception during transmission could arguably support a conclusion that Salman retained a reasonable expectation of privacy in the communications before they reached the third-party recipient, there is no indication that collection of the information at issue in this motion occurred through government interception of communications. Additionally, defendant has clarified that she does not challenge the underlying seizure and extraction of the phones. Thus, in contrast to the emails at issue in *Hasbajrami II*, the information stored in the NMEC database was not collected as a result of government interception, and Salman has not otherwise articulated a basis on which the Court could conclude that she has a reasonable expectation of privacy in any information stored in the NMEC database, or in the data returned from querying the database.

Thus, while a query of the NMEC database may constitute a "Fourth Amendment event," the Court need not reach that question, as defendant has failed to articulate an expectation of privacy in any of the information contained in the NMEC database, or in

the database itself.<sup>8</sup> As defendant has failed to articulate a reasonable expectation of privacy, she has failed to establish standing under the Fourth Amendment. Accordingly, her motion to suppress is denied.

### CONCLUSION

For the reasons stated above, defendant's motion to suppress evidence derived from queries of the NMEC database is DENIED.

**SO ORDERED.**

/s/ Natasha C. Merle  
NATASHA C. MERLE  
United States District Judge

Dated: November 5, 2025  
Brooklyn, New York

---

<sup>8</sup> Additionally, in support of her argument that a querying a database implicates her Fourth Amendment rights, defendant points to the Supreme Court's decision in *United States v. Carpenter*, 585 U.S. 296, which held that a warrant is generally required to obtain cell-site location information from a service provider. Defendant argues that a search of the NMEC database is "akin to the unrestricted access to a database that the Court was unwilling to sanction in *Carpenter*." Mot. 12–13. However, the cell-site location information at issue in *Carpenter* allowed the government to recreate the defendant's location over the course of 127 days by obtaining that information directly from the cell-service provider, and the Court concluded that the defendant had a privacy interest in that data. *See Carpenter*, 585 U.S. at 313 ("[W]hen the Government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements."). Here, the Court has found that the defendant has not articulated a reasonable expectation of privacy in the information at issue. The Court in *Carpenter* also cautioned that its decision was "a narrow one" that did not "consider other collection techniques involving foreign affairs or national security," *id.* at 316, both of which are at issue here.